TRUST Science & Technology Center

Team for Research in Ubiquitous Secure Technology

Larry Rohrbough
TRUST Executive Director
University of California, Berkeley

California Office of Information Security
CISO Lecture Series

February 25, 2010 | Sacramento, California

Outline

- TRUST Overview
- TRUST Research
- TRUST Education and Diversity
- TRUST Knowledge Transfer
- Summary

Outline

- TRUST Overview
- TRUST Research
- TRUST Education and Diversity
- TRUST Knowledge Transfer
- Summary

TRUST Overview

TRUST
Team for Research in Ubiquitous Secure Technology

National Science Foundation Science & Technology Center (STC) Program

Science & Technology Center (STC) established in 1987 to fund **important basic research and educational** activities and to **encourage technology transfer** and innovative approaches to **interdisciplinary problems**.

Per NSF, the STC Program:

- "Enables *innovative research and education* projects of national importance…"
- "Requires a *Center mode* of support to achieve the goals…"
- "Conducts world-class research in *partnerships*…"
- "Creates new and meaningful knowledge of significant *benefit to society*…"

National Science Foundation
WHERE DISCOVERIES BEGIN

Office of Integrative Activities (OIA)

Directorate for Computer & Information Science & Engineering (CISE)

NSF Center Funding
(FY2005 - 2015)

$40M ($4M/Year, 10 Years)

TRUST Overview (cont.)

TRUST: Team for Research in Ubiquitous Secure Technology

TRUST MISSION

S&T that will radically transform the ability of organizations to *design*, *build*, and *operate* trustworthy information systems for critical infrastructure

Center Approach

- Address fundamental cyber security and critical infrastructure protection problems of national importance
- Tackle "Grand Challenge" scale integrative research projects
- Include external (including international) collaboration for research project sponsorship and technology transition

Supporting Personnel

Graduate Students	100
Faculty	53
Research Scientists	10
Staff/Other	9
Undergrad Students	8
Post Doctorates	6
TOTAL:	**186**

Affiliated Institutions

Berkeley – University of California
Carnegie Mellon
Cornell University
Mills College
San José State University
Smith College
Stanford University
Vanderbilt University

Supporting Disciplines

- Computer Engineering
- Computer Science
- Economics
- Electrical Engineering
- Law
- Public Policy
- Social Science

TRUST Overview (cont.)

TRUST
Team for Research in Ubiquitous Secure Technology

Center Structure: Core Research with Integrated Education and Knowledge Transfer

To achieve the TRUST mission and objectives, Center activities are focused in three tightly integrated areas…

Education/Diversity

Curriculum development and teaching the next generation of computer / social scientists and engineers

TRUST Academy Online

Textbooks

SECuR-IT

WISE

SUPERB-IT

TRUST Seminar

Research

Interdisciplinary projects combine fundamental science and applied research to deliver breakthrough advances in trustworthy systems

Financial Infrastructures

- Web browser/server security
- Botnet and malware defenses
- Secure software infrastructure

Health Infrastructures

- Privacy Modeling and Analysis
- HIS/Patient Portal Architectures
- Patient Monitoring Sensors

Physical Infrastructures

- Embedded systems for SCADA and control systems
- Sensor networks for Demand Response systems
- Information privacy/security

Knowledge Transfer

Dissemination and transition of Center research results and collaboration opportunities with external partners

BT CISCO hp intel Microsoft Sun microsystems TATA United Technologies TATA CONSULTANCY SERVICES

U.S. DEPARTMENT OF HOMELAND SECURITY AFRL THE AIR FORCE RESEARCH LABORATORY LEAD | DISCOVER | DEVELOP | DELIVER

iCAST
International Collaboration for Advancing Security Technology

Outline

- TRUST Overview
- TRUST Research
- TRUST Education and Diversity
- TRUST Knowledge Transfer
- Summary

TRUST Research

TRUST Team for Research in Ubiquitous Secure Technology

Grand Challenge #1: Financial Infrastructures

Scope and Objectives:

Trustworthy environment that links and supports commercial transactions among financial institutions, online retailers, and customers.

Fundamental Challenges:

- Systems Not Under Control of One Organization
  - Web browsers are separately administered by non-experts
  - Intra-enterprise financial infrastructure highly networked
- Systems Involve Computers and People
  - Web site wants to authenticate a person, not a machine
  - No control over end-user actions and decisions
  - If browser indicates “buy”, is it from the user?
- Rapid Evolution of World-Wide Systems
  - Open-source browser, server, handheld platforms
  - Complex regulatory (e.g., SOX) and competitive environment

TRUST Research and Development:

- Secure application and network infrastructure (front/back end)
- Detection, defenses, and forensics of malware, botnets, spyware, and other online attacks
- Authentication of client to site and site to client
- Design and construction principles for secure web systems
- Security risk management, economics of security, behavioral studies, end-user issues

"Go where the money is...and go there often."
Willie Sutton

TRUST Research (cont.)

TRUST
Team for Research in Ubiquitous Secure Technology

Grand Challenge #2: Health Infrastructures

LEADING CAUSES OF DEATH[1]

Diseases of the Heart	726,974
Cancer (malignant neoplasms)	539,577
Cerebrovascular Disease	159,791
Chronic Obstructive Pulmonary Disease	109,029
Medical Errors[2]	**44,000–98,000**
Accidents and Adverse Effects (motor vehicle accidents = 43,458; all others = 52,186)	95,644
Pneumonia and Influenza	86,449
Diabetes	62,636
Suicide	30,535
Kidney Disease	25,331
Liver Disease	25,175

SOURCES: 1. Centers for Disease Control and Prevention, 1997. 2. IOM, *To Err Is Human: Building a Safer Health System*, 2000.

TRUST Research (cont.)

TRUST Team for Research in Ubiquitous Secure Technology

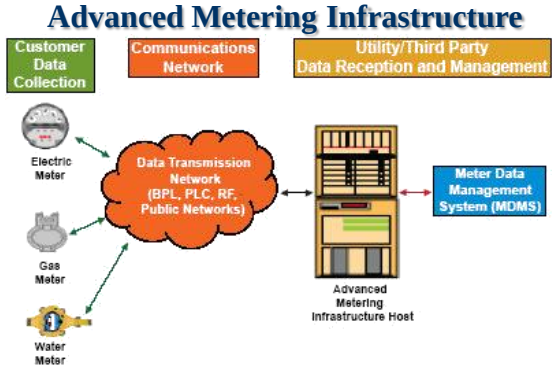
Grand Challenge #3: Physical Infrastructures

Scope and Objectives:

Advances that support next generation Supervisory Control and Data Acquisition (SCADA) and Distributed Control Systems (DCS), including for power, water, telecom, and address privacy issues.

Fundamental Challenges:

- Protecting Immense Investment
  - Financial: Sunk costs and ongoing development and maintenance
  - Human: Established development, maintenance, and regulatory organizations at federal and state levels
- Critical to National Economy
  - Modes of production depend on functionality of these systems
  - Multiple externalities have created system dependencies (e.g., air traffic control dependence on power and telecom infrastructure)
- Increasing Infrastructure Complexity
  - As systems evolve, need to ensure adequate control, security, and privacy (as well as securing legacy systems…)



TRUST Research and Development:

- Security threat models (external and insider attacks)
- Secure control and intrusion resilience
- Novel sensor networking technologies for control and maintenance
- Privacy-preserving demand response systems, especially for residential consumers

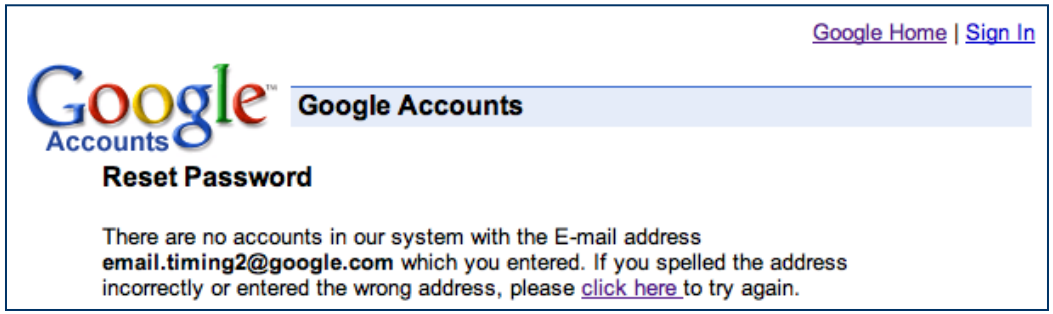
TRUST Research (cont.)

TRUST
Team for Research in Ubiquitous Secure Technology

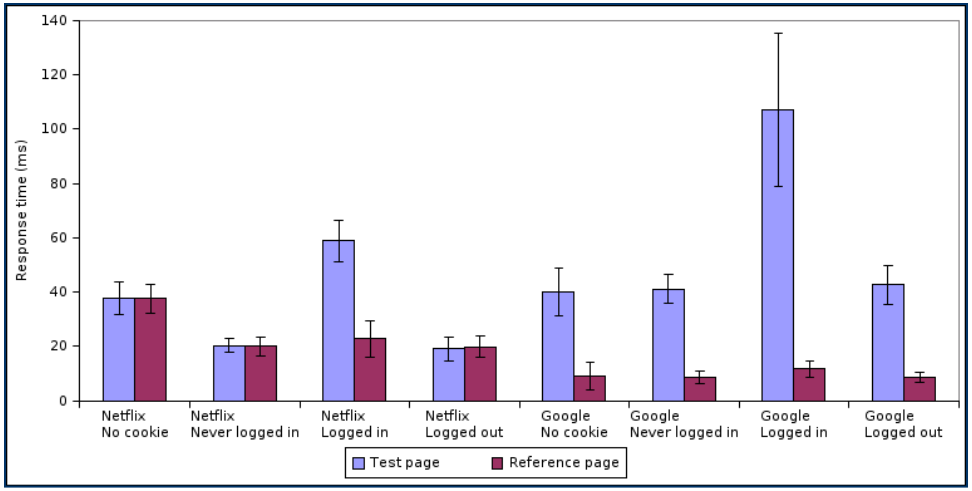
Research Highlight: Financial Infrastructures

Exposure of Private Information via Website Timing Attacks

- Most sites have "Forgot my password" pages



- These pages may leak whether an e-mail is valid at that site
  - Identified through outreach to financial services company
  - Vulnerability found on virtually every site tested
  - TRUST communicated results, repair adopted, work published



Bortz, Boneh, Nandy
16th International World Wide Web Conference (WWW2007)

TRUST Research (cont.)

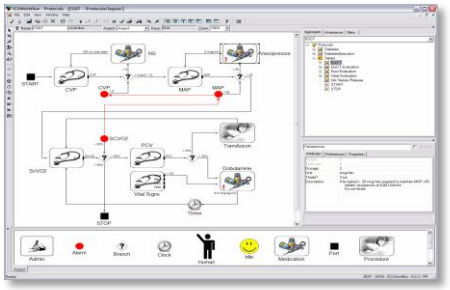
TRUST
Team for Research in Ubiquitous Secure Technology

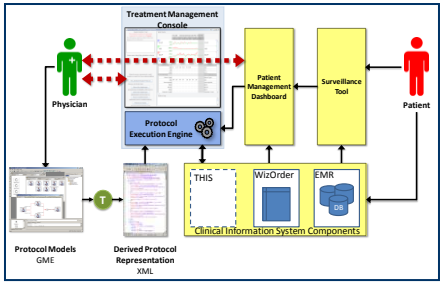
Research Highlight: Health Infrastructures

Sepsis Treatment Enhanced through Electronic Protocolization (STEEP)

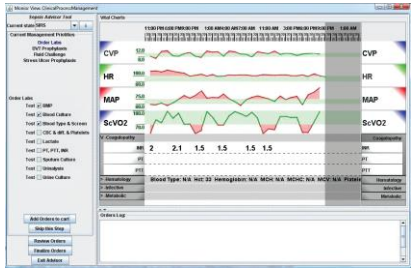
- **Hypothesis**
  - Implementation of an electronic process management tool will result in increased adherence to *evidence-based practices*, improvement in objective *quality indicators*, and *better clinical outcomes*.
- **Sepsis**
  - Common: ~750,000 cases/year
  - Deadly: ~25-35% mortality rate
  - Expensive: $17B/year (40% of ICU costs)
  - Treatable: Validated treatment protocols
- **Challenges**
  - Operational protocols, healthcare policies, and treatment guidelines are rarely phrased in a mathematically sound manner
  - Semantics of the protocol modeling language
  - Validation /verification of protocol models
  - Integration with Clinical Information Systems
  - Clinical barriers to adoption

- **Model-Based Approach**
  - Complexity of these systems is a major concern.
  - Model verification for security and privacy properties of the modeled architecture.
  - Models are protocol-driven, evidence-based, customizable, and integrated.





- **Development and Deployment**
  - STEEP Treatment Management Console (TMC), which shows recommended actions and displays patient health information.
  - Deployed at the Vanderbilt University Medical Center



Mathe, Ledeczi, Nadas, Sztipanovits, Martin, Weavind, Miller, Miller, Maron
"A Model-Integrated, Guideline-Driven, Clinical Decision-Support System", *IEEE Software*, July/August 2009

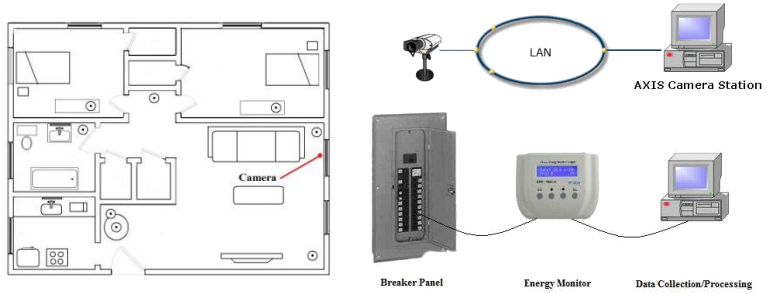
TRUST Research (cont.)

TRUST Team for Research in Ubiquitous Secure Technology

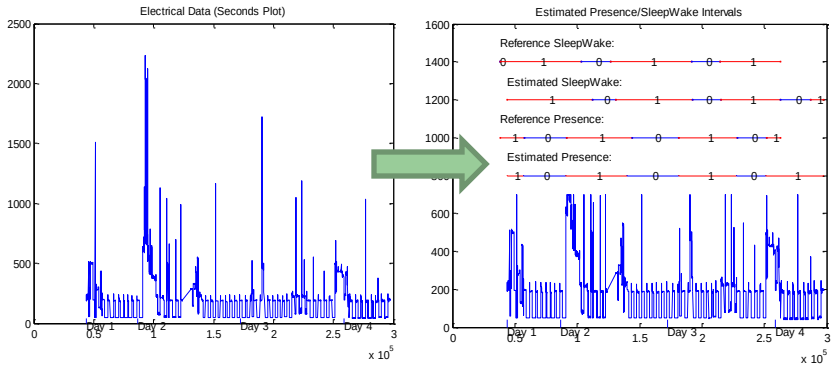
Research Highlight: Physical Infrastructures

Privacy Concerns in Upcoming Demand Response Systems

- Next generation demand-response architectures
  - Advantages: cost savings, increased grid reliability, new modes of consumer-utility interaction.
  - Disadvantage: Increased availability of data creates privacy/security issues.
  - Claim: Detailed household consumption data gathered by AMIs can reveal personally identifying information.
  - Goal: Metric which associates the degree of data availability with potential privacy risks, providing a robust and reliable indicator
- Field Experiment
  - Energy-usage monitors and cameras
  - Behavior-extraction algorithms to determine Presence/Absence, Appliance Use, and Sleep/Wake Cycle.



- Findings
  - Smart Metering Provides Data Equivalent to a "Search": Algorithms perform well in determining presence and sleep cycles—over 90% of total interval length was correctly classified.



Lisovich, Mulligan, Wicker
"Inferring Personal Information from Demand-Response Systems", *IEEE Security & Privacy*, January/February 2010

Outline

- TRUST Overview
- TRUST Research
- TRUST Education and Diversity
- TRUST Knowledge Transfer
- Summary

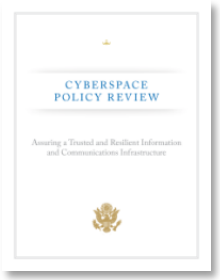
TRUST Education and Diversity

TRUST
Team for Research in Ubiquitous Secure Technology

Education and Human Resource Development Challenges

"To ensure that federal cyber policies enhance our security and our prosperity…we're making ***a new commitment to education in math and science, and historic investments in science and research and development***. "

President Barack Obama, May 29, 2009



Cyberspace Policy Review

"Expand support for key education programs and research and development to ensure the Nation's continued ability to compete in the information age economy."

"Develop a strategy to expand and train the workforce, including attracting and retaining cybersecurity expertise in the Federal government."

Cyber IN-security: Strengthening the Federal Cybersecurity Workforce

"Develop a government-wide strategic blueprint to acquire, train, and retain the cybersecurity talent the federal government needs."

"Provide significant funding to develop and keep federal cybersecurity talent knowledgeable at a 'state of the art' level of readiness through training and development."

"Ensure adequate funding of successful programs that provide graduate and undergraduate scholarships in the cybersecurity field."

TRUST Education and Diversity (cont.)

TRUST
Team for Research in Ubiquitous Secure Technology

Diverse Set of Education and Outreach Activities

Programs focused on integrating trustworthy technologies, systems, and policy into learning opportunities for a broad range of participants

TEACHING/TRAINING

New Courses

- Foundational topics such as computer security, network security, software security.
- Emerging topics such as web programming and security, data privacy in biomedicine.
- Domain-specific topics such as security of electric energy systems

New Graduate Specialization

- Developing an MS/PhD research area in *Cyber Security and Trustworthy System* at all TRUST partner institutions

Professional Development

ebay, RAPPORT, Sun microsystems, hp, Salesforce, YAHOO!

DISSEMINATION

TRUST Academy Online

https://tao.truststc.org

TRUST Security Seminar

DIVERSITY

San José State University
Alliance for Minority Participation

HBCU Summer Partnership

H&SS Information Systems
Carnegie Mellon

SUPERB-IT

Women's Institute in Summer Enrichment

TRUST Education and Diversity (cont.)

TRUST
Team for Research in Ubiquitous Secure Technology

Example New and Enhanced Academic Courses (Undergraduate + Graduate)

Educate the next generation of computer scientists, engineers, lawyers, policy makers, and social scientists in cyber security and trustworthy systems

Course Title	Program Level	Campus	Offered	Enrollment
Software Security Technologies (CMPE279)	Graduate	SJSU	2009	50
The Digital World and Society (CMPE025)	Lower Division	SJSU	2009	20
Web Programming and Security (CS142)	Lower Division	Stanford	2009	100
Internet Policy Challenges in a Global Environment (INF290)	Graduate	Berkeley	2009	15
Mobile Communications (ECE5680)	Graduate	Cornell	2009	50
Information Technology in Society (CS39M)	Freshman	Berkeley	2008	25
TechLaw with Progressive Minds (CS302)	Graduate	Stanford	2008	20
Electric Energy Systems (EGR 325)	Upper Division	Smith	2007	12
Data Privacy in Biomedicine (BMIF380/CS396)	Graduate	Vanderbilt	2007	5
Fault-tolerant Distributed Computer Systems (CS514)	Upper Division	Cornell	2007	80
Sensor Networks (ECE7940)	Graduate	Cornell	2007	20
System Security (CS5430)	Upper Division	Cornell	2006	80
Introduction to Security and Policy (CEC18-630)	Graduate	CMU	2005	80
Network Security (18-731)	Graduate	CMU	2005	80
Computer Security (CS161)	Upper Division	Berkeley	2005	80
Network Security (CS291)	Upper Division	Vanderbilt	2005	15

TRUST Education and Diversity (cont.)

TRUST
Team for Research in Ubiquitous Secure Technology

TRUST Graduate-Level Security Specialization

MS/PhD research area in *Cyber Security and Trustworthy System* at all TRUST partner institutions

EECS Research Area begun at UC Berkeley in 2007
(http://eecs.berkeley.edu/Research/Areas/SEC)

- Enhanced Curriculum Development
  - Create five new courses in trustworthy systems: Pilot at UC Berkeley
    - Internet Technologies
    - Societal and Ethical Implications of Trustworthy Systems
    - Security and Computer Forensics
    - Internet Law
    - IT consulting and professional services
  - Cross-listed with the College of Engineering, School of Information, and the School of Law
- MS/PhD Program Specialization in Security
  - Open to all graduate level students
  - Leverage existing graduate-level courses + new courses offering
  - Will increase security exposure across TRUST institutions

TRUST Education and Diversity (cont.)

Summer Programs: Research Experiences for Undergraduates

- Program Overview
  - 8-week research experience guided by faculty mentors and graduate students
  - Educational activities include lab tours and industry field trips
  - Graduate school advising and subsidized GRE prep course
  - $4,000 Stipend + travel allowance + room and board provided
- Program Impact
  - 2006-2008: TRUST hosted 18 undergraduate students
    - 72% female/39% URM
    - 100% U.S. persons
    - 94% in grad school or applying
  - 2009: TRUST hosted 10 students
  - 2010: TRUST hosting 28 students (across five TRUST institutions)

- Participant Testimonial

  "The best part was the exposure to both the academic and industrial pathways. Without the first-hand company seminars and research experience I gained from the program, I would have made a much weaker decision as in which path to choose!"

- More Information Online
  - **Program Description at:**
    `https://www.truststc.org/reu/`

TRUST Education and Diversity (cont.)

TRUST Team for Research in Ubiquitous Secure Technology

Summer Programs: Security Summer Internship

SECuR-IT : Summer Experience, Colloquium, and Research in Information Technology

- Program Overview
  - 10-week graduate student summer program in computer security
  - Paid internship at a Silicon Valley technology company
  - Housing at San Jose State
  - Seminars in security related topics
  - College units for summer educational program
  - Program funded by industry partners
- SECuR-IT Interns

- Participating Companies

eBay PayPal RAPPORT Salesforce Sun microsystems YAHOO!

- Participant Testimonials

"SECuR-IT was a great combination classes and work! Loved all of it!"

"The eBay internship program is great! I enjoyed it very much! This is my best summer ever, both on learning and having so much fun!"

- More Information Online
  - **Program Description at:**
    `https://www.truststc.org/securit/`

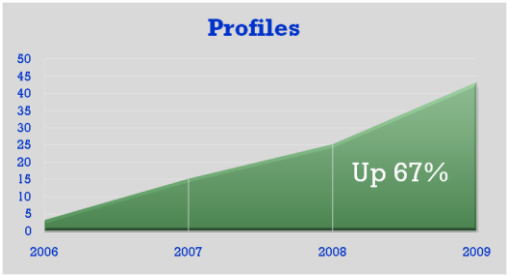
TRUST Education and Diversity (cont.)

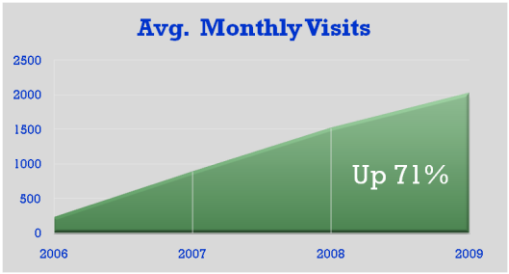
TRUST Academy Online (TAO)

Back-end repository and web-based portal for collecting an disseminating learning material to faculty and researchers working in TRUST-related areas

- TRUST research materials become module content and project profiles on the TAO
- TAO contains teaching modules that can be incorporated into diverse curricula (e.g., privacy modules for engineers working on SCADA control systems; cryptography modules that introduce DRM concepts to law students)

https://tao.trusstc.org





Outline

- TRUST Overview
- TRUST Research
- TRUST Education and Diversity
- TRUST Knowledge Transfer
- Summary

TRUST Knowledge Transfer

TRUST
Team for Research in Ubiquitous Secure Technology

External Partners/Sponsors Support Technology Transition

OBJECTIVE

Transition security, privacy, and infrastructure protection research to *industry*, *government agencies*, and *international partners* to promote the use and evolution of ubiquitous secure technology

Industry Partners

BT, IBM, Sun microsystems, Cisco, Intel, Symantec, NTT DoCoMo, Microsoft, Tata, Tata Consultancy Services, EADS, Oak Ridge National Laboratory, Telecom Italia, HP, Qualcomm, United Technologies

Government Sponsors

NSF, National Security Agency, Air Force Office of Scientific Research, DARPA, U.S. Department of Homeland Security, AFRL – The Air Force Research Laboratory

International Collaborators

iCAST – International Collaboration for Advancing Security Technology

CSIT – Centre for Secure Information Technologies

Amrita-TIFAC Core in Cyber Security

TRUST Knowledge Transfer (cont.)

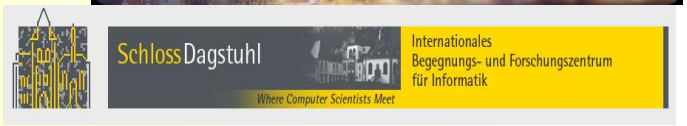
TRUST
Team for Research in Ubiquitous Secure Technology

Industry: Adoption/Use of Center Research Results by Commercial Partners

Use and evolution of ubiquitous secure technology via transition of TRUST research to commercial companies and other partners

Electronic Medical Records

- Model-Based Trustworthy Health Information Systems (MOTHIS) 2007 & 2008 and Dagstuhl 2009: US and EU technologists + medical/legal/policy experts
- Adoption of model-based methods for HIS (architectures, privacy and security policies, security mechanisms, web authentication, and human factors)
- DexterNet – Body sensor network for patient monitoring and in-home healthcare.



Vanderbilt Home Care
Hearts and Minds at Home

TELECOM ITALIA

PINE

End User Security

- Identity theft (anti-phishing) and authentication/verification web browser tools
- Malware detectors (Minesweeper, Panorama) and botnet zombie detection system (BotSwat)

RSA SECURITY

Google Code

Adobe

vmware

Sun microsystems java

Network Defenses

- Network intrusion detection and monitoring technology
- Portcullis/SNAPP – High network availability during massive attacks (e.g., DDoS)

財團法人資訊工業策進會
INSTITUTE FOR INFORMATION INDUSTRY

amazon.com

TRUST Knowledge Transfer (cont.)

TRUST
Team for Research in Ubiquitous Secure Technology

Government: Technology + Policy Advising

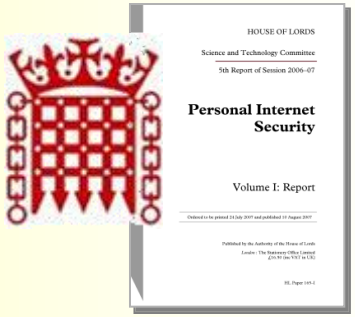
Advising and shaping policy and legislation at the Federal, State, and Local government level (US) as well as working with international governments

US Federal/State/Local

- Privacy implications of residential demand-response systems
- Federal Trade Commission identity management best practices
- Data Breach Notification laws expanded from California (SB 1386) to 39+ states
- Privacy and security vulnerabilities of RFID and end-user comprehension of real and perceived risks

UK House of Lords

- Science and Technology Committee visit to UC Berkeley March 2007
- TRUST briefings on *Network Monitoring*, *Data Breach Notification*, *Telecommunications Legal Issues*, and *Industry/Academic Partnerships*



Taiwan Science & Technology Advisory Group

- Reviewer on STAG panel investigating Taiwan's "Information-Communication Security" capabilities, August 2009
- Topics: global competitiveness, industry, education, e-government/e-commerce, health/medical

行政院科技顧問組
Science and Technology Advisory Group of Executive Yuan

TRUST Knowledge Transfer (cont.)

TRUST
Team for Research in Ubiquitous Secure Technology

Department of Defense: Security Research + Experimentation + Advising

Security technology to enhance national defense, improve infrastructure networks and systems, and address the growing threat of cyber attacks

Air Force Office of Scientific Research / Research Laboratory

- Secure the Global Information Grid (GIG) and improve security for Network Centric Enterprise Systems (NCES)
- Time-criticality/quality of service with COTS and web services
- Legacy application/system-of-system information assurance
- Secure and dynamic service discovery and mediation

AF-TRUST
Air Force Team for Research in Ubiquitous Secure Technology

AFRL
THE AIR FORCE RESEARCH LABORATORY
LEAD | DISCOVER | DEVELOP | DELIVER

Defense Advanced Research Projects Agency

- Desire for large-scale cyber network testing & evaluation
- Possibly build on Berkeley/USC-ISI cyber testebed (DETER) architecture
- Leverage experimentation experience of TRUST DETER team

deterlab
based on emulab

DARPA

Scientific Advisory Boards / Strategic Studies Groups

- Implications of Cyber Warfare (2007)
- Cyberspace and Maritime Operations in 2030 (2007)
- Defending and Operating in a Contested Cyber Domain (2008)

TRUST Knowledge Transfer (cont.)

TRUST
Team for Research in Ubiquitous Secure Technology

International: U.S / Taiwan Partnership for Advancing Security Technology

NTUST

iCAST
International Collaboration for Advancing Security Technology

TWISC Taiwan Information Security Center

Industrial Technology Research Institute

Berkeley
UNIVERSITY OF CALIFORNIA

Carnegie Mellon

OBJECTIVE:

Joint U.S./Taiwan R&D of security technologies for cryptography, wireless networking, network security, multimedia security, and information security management.

PARTNERSHIP:

- *3-year collaboration agreement (2006-2009)*
- *U.S. $2M per year investment by Taiwanese government*
- *Joint research and publications*
- *Prototyping and proof-of-concept for Taiwanese and U.S. industry*
- *Student/faculty exchange program*

RESEARCH:

- *Security for Pervasive Computing*
- *Trusted Computing Technologies*
- *Wireless Security*
- *Sensor Network Security*
- *Intrusion Detection and Monitoring*

Outline

- TRUST Overview
- TRUST Research
- TRUST Education and Diversity
- TRUST Knowledge Transfer
- Summary

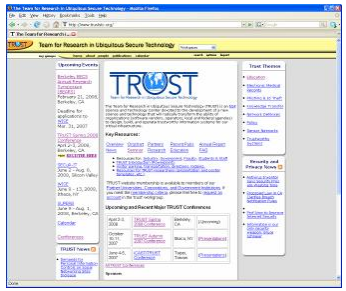
Summary

- TRUST is addressing challenge of building trustworthy systems
  - Multi-disciplinary team addressing fundamental cyber security and infrastructure problems of national importance.
  - Researchers at the forefront many emerging cyber threats (ID theft, data breaches, cyber attacks, malware, botnets, …).
- TRUST hallmark and legacy
  - Results of large, integrative **research** projects.
  - Comprehensive **education** program to groom the next generation of cyber security/privacy researchers and professionals.
  - Successful **knowledge transfer** of results—technology adoption, policy/legal reforms, researcher/practitioner community building.
- TRUST opportunities
  - Looking for new ideas and collaborators in government and industry.
  - Looking for hard problems to solve and applications for Center research.
  - Interested in sharing lessons learned for making an Academic/Government/Industry model successful

Thank You!

Contact Information

Larry Rohrbough
Executive Director
TRUST Science and Technology Center
University of California, Berkeley
+1 510-643-3032 (Work)
+1 703-328-5221 (Mobile)
larryr@eecs.berkeley.edu



www.truststc.org